**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06 — A1

(11) International Publication Number: **WO 00/67447**

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/IE00/00050

(22) International Filing Date: 2 May 2000 (02.05.00)

(30) Priority Data:
S990359 29 April 1999 (29.04.99) IE

(71)(72) Applicants and Inventors: BLEAHEN, Michael [IE/IE]; 38 Ashfield Road, Ranelagh, Dublin 6 (IE). WALLER, William [IE/IE]; 38 Ashfield Road, Ranelagh, Dublin 6 (IE). FAHEY, Paraic [IE/IE]; 38 Ashfield Road, Ranelagh, Dublin 6 (IE).

(74) Agent: MACLACHLAN & DONALDSON; 47 Merrion Square, Dublin 2 (IE).

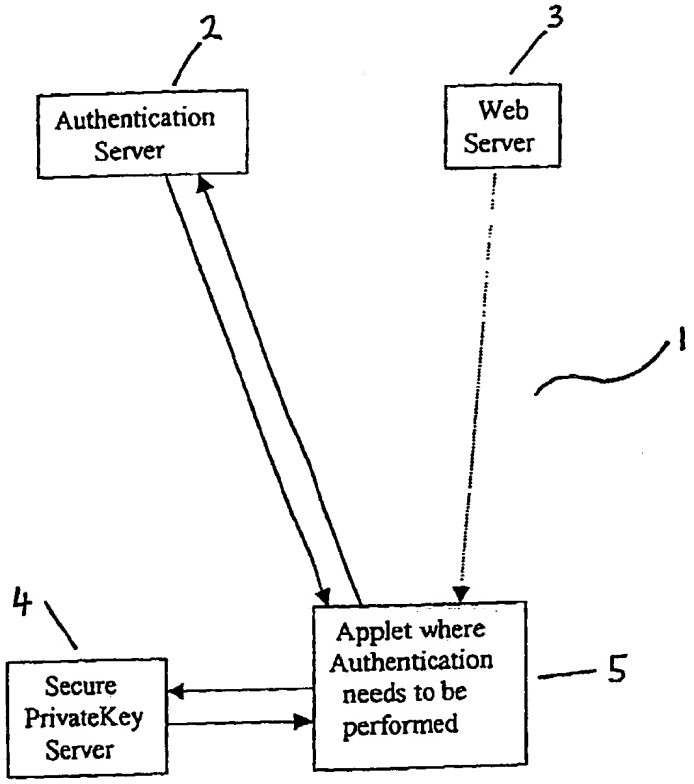
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: IMPROVEMENTS IN AND RELATING TO SECURE DATA TRANSMISSION

(57) Abstract

A method for secure data communication for use in an electronic commerce environment of the type having an authentication server (2), a web server (3) and an applet (5). Data communications between the authentication server, web server, applet and a secure private key server (4) is controlled by generating a certificate–received signal, initiating an authentication request, requesting a server authentication certificate, extracting the vendor public key, loading a client certificate into the applet and simultaneously transmitting the client certificate to the authentication server and receiving the client certificate at the authentication server and extracting a client public key from the client certificate and simultaneously extracting the client public key from the client certificate. This overcomes the problems associated with allowing a vendor access to a users private key.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

# IMPROVEMENTS IN AND RELATING TO SECURE DATA TRANSMISSION

The present invention relates to a secure data transmission and in particular to a method for ensuring the authenticity and privacy of data transmission between two or more computer systems.

The business of selling products and services across communication channels, such as the Internet, is now generally referred to as electronic commerce or "E-Commerce". Security and responsiveness are the principal concerns for users in all Ecommerce transactions. To provide this security, cryptography is normally used. Traditionally in cryptography, the sender and receiver of a data message both know and use the same secret key. The sender uses the secret key to encrypt the message and the receiver decrypts the message using the same secret key. This is known as symmetric cryptography. Symmetric cryptography requires the sender and receiver to agree on the secret key without a third party discovering the key. This can prove problematic when the sender and receiver are in separate physical locations, as a transmission medium, which cannot always be guaranteed, is required to communicate the secret key. If a third party intercepts the key in transit they can use the key to read, modify, or forge messages encrypted or authenticated using that key. This destroys user confidence in the transmission system and is therefore not ideally suited to Ecommerce applications.

To overcome this problem, public-key cryptography has been developed. Public-key cryptosystems have two primary uses, encryption and digital signatures. In a public-key cryptosystem, used for encryption, sender and receiver each have a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated as all data communications involve only public keys and no private key is ever transmitted or shared greatly increasing the trust level in the overall system. Public keys must, however, be associated with their users in an authenticated manner. In these types of systems, anyone can send a confidential message by just using public information and the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. The problem with this system is that the private key is of

necessity, linked mathematically to the public key. Therefore, it is always possible to attack a public-key system to derive the private key from the public key. Typically, the defence against this is to make the problem of deriving the private key from the public key as difficult as possible. For example, many public-key cryptosystems are designed so that deriving the private key from the public key requires the attacker to factor a large number, it which case it is computationally infeasible to perform the derivation.

As indicated above, public-key cryptography can also be used for authentication often referred to as digital signatures. To sign a message, a sender performs a computation involving both the sender's private key and the data message. The output is called a digital signature and is attached to the message. To verify the signature, the recipient does a computation involving the data message, the purported signature, and the sender's public key. If the result is correct according to a simple, prescribed mathematical relation, the signature is verified to be genuine, otherwise, the signature is fraudulent or the message may have been altered.

A number of solutions to various aspects of public-key cryptosystems are known. For example, US Patent Nos. US 4,200,770 and US 4,218,582 (Hellman et al) show encryption as well as a means of authentication using long-term public keys as does US Patent No. 4,405,829 (Rivest et al). All of the proposed solutions provide a high level of security, however, as Ecommerce develops it is increasingly required that the senders private key be taken into a Vendor's software applet in an Ecommerce transaction to authenticate the purchase. The greatly reduces the consumers confidence in such transactions as the security of the private key is now in the hands of the vendor and beyond the control of the user. Additionally, it is possible to create code to transparently extract the private key and subsequently use the key for unauthorised transactions.

In an attempt to further enhance the security limitations described above, certification and certificates have been developed. These certificates allow for the possibility of accessing other public keys and making public one's own public key in a manner, which allows legitimate retrieval of public keys but prevents impersonation. Such certificates require authentication of the identity and the public key of an individual before issuing a

certificate. Even using such certificates, users are still required to store their private keys securely, so no intruder can obtain them, yet the keys must be readily accessible for legitimate use. Therefore, passing a private key for authentication to a vendor fundamentally compromises system integrity in a manner, which is unacceptable to most users.

There is therefore a need for method for secure data communication, which will overcome the aforementioned problems.

Accordingly, there is provided a method for secure data communication for use in an Ecommerce environment of the type having an authentication server, a web server and an applet, the method controlling data communications between the authentication server, web server, applet and a secure private key server, the method performing the steps of: -

downloading the applet from a vendor web site in response to a data communication request;

requesting a copy of a vendor certificate from the web site;

extracting a data response to generate a certificate-received signal;

automatically initiating an authentication request for transmission to the authentication server;

interrogating the authentication server and requesting return transmission of a server authentication certificate;

transmitting a vendor certificate to the applet;

automatically extracting the vendor public key from the vendor certificate within the applet;

loading a client certificate into the applet and simultaneously transmitting the client certificate to the authentication server; and

receiving the client certificate at the authentication server and extracting a client public key from the client certificate and simultaneously automatically extracting the client public key from the client certificate by the applet.

Preferably, the method comprises the further steps of: -

initialising the secure private key server;

loading a certificate into the secure private key server;

loading a client private key into the secure private key server;

generating an auto authenticate signal for transmission to the authentication server requesting initialisation of a new authentication process;

retrieving a predefined text string from a local memory using the authentication server and encrypting the text string to generate a cipher text string using the client public key on receipt of the authenticate signal;

transmitting a cipher text string to the applet, receiving the cipher text string from the authentication server and routing the cipher text string to the secure private key server;

decrypting the cipher text string to extract a decrypted text string using the client private key and transferring the decrypted text string to the applet;

encrypting the decrypted text string received from the secure private key server with the vendor public key extracted from the vendor certificate to generate a vendor encoded text string;

sending the vendor encoded text string to the authentication server, decrypting the encoded text string to generate an authentication text string using the vendor private key; and

comparing the authentication text string and the predefined text string to generate a match / no match signal and in response to a no match signal terminating communication or in response to a match signal for further authenticated data communications.

According to another aspect of the invention there is provided a method of generating a certificate operating in a data communication system having a web server, a certification authority, an applet and a secure private key server the method performing the steps of: -

gathering certification information in the applet and transmitting the information to the secure private key server;

generating a key pair in the secure private key server on receipt of the packaged information and a certificate created using the generated key pair; and

returning the certificate to the applet for onward transmission to the certification authority for signature.

The invention will now be described with reference to the accompanying drawings, which show, by way of example only, a method for secure data communication in which: -

Fig.1 is a block diagram showing an Ecommerce environment implementing a method for secure data communication in accordance with the invention; and

Fig.2 is a block diagrammatic view of a method of generating a certificate for use in the invention.

Referring to the drawings and initially to Fig.1 there is shown a block diagram illustrating a method for secure data communication in accordance with the invention indicated generally by the reference numeral 1. In order to aid clarity, references to specific computer systems, performance details, communications media, protocols, timing, ports and the like have been omitted. It will be appreciated, by those skilled in the art, that the invention may be implemented in a large number of ways including software, firmware or incorporation in an electronic commerce chip (ECC) without departing from the scope of the invention. An exhaustive recitation of possibilities would only serve to unnecessarily obscure the current invention.

The method for secure data communication 1 is illustrated in use in an Ecommerce environment having an authentication server 2, a web server 3, a secure private key server 4 and an applet 5.

In operation, the method begins by downloading the applet 5 from a vendor web site in response to a data communication request to purchase a service or product. The applet 5 then requests a copy of the vendor's certificate from the web site. Upon receiving a data response from the web site the certificate is extracted to generate a certificate-received signal. The certificate-received signal causes the applet to automatically initiate an authentication request, transmitted to the vendor's authentication server. This authentication request interrogates the authentication server and requests return transmission of a server authentication certificate. When this sequence has been completed without transmission error, the vendor then transmits a vendor certificate to the applet. The vendor's public key is automatically extracted from the vendor certificate within the applet upon receipt. The client then loads a client certificate into the applet and simultaneously transmits the client certificate to the authentication server. The Authentication Server receives the client certificate and extracts a client public key from the client certificate. At the same time, the client public key is automatically extracted from the client certificate by the applet.

Once these steps have been successfully completed, authentication begins by initialisation of the secure private key server 4. The client loads his/her own certificate into the secure

private key server. A client private key is then loaded into the secure private key server 4 generating an auto authenticate signal for transmission to the authentication server requesting initialisation of a new authentication process.

The authentication server retrieves a predefined text string from a local memory and encrypts the text string to generate a cipher text string using the client public key on receipt of the authenticate signal. This cipher text string is then transmitted to the applet for further processing. The applet receives the cipher text string from the authentication server and routes the cipher text string to the secure private key server.

When the secure private key server receives the entire cipher text string it decrypts the cipher text string to extract a decrypted text string using the client private key. The decrypted text string is then transferred to the applet.

The applet in turn encrypts the decrypted text string received from the secure private key server with the Vendor public key extracted from the vendor certificate described above to generate a vendor encoded text string.

The vendor encoded text string is then sent to the authentication server for processing. When the encoded text string is received it is immediately decrypted to generate an authentication text string using the vendor private key. A comparison is then performed between the authentication text string and the predefined text string from a local memory to generate a match / no match signal. If a no match signal is generated, data communication is terminated, however, a match signal shows that the client has been authenticated and the client can proceed to use the applet for further data communications.

In this way, the private key critical to such data communication is never beyond the user's control enhancing confidence in the overall communication system. As the private key is never stored on a vendors system it is not susceptible to attacks from individuals intent on fraudulent use of the key.

It will be understood that when the invention is enacted in software that the code required is minimal by comparison with currently available alternatives. Additionally, to further

promote consumer confidence in the security of the private key, it is intended to supply source code, which may be compiled by the user. This will allow customers to view the code and ensure no unauthorised caching or transmission of the private key occurs.

Referring now to Fig. 2 there is illustrated a method of generating a certificate for use in the invention indicated generally by the reference numeral 20. The method 20 operates in a data communication system having a web server 21, a certification authority 22, an applet 23 and a secure private key server 24.

In use to produce a certificate, the applet 23 gathers the required information about the person or entity requesting certification. When the applet has gathered the necessary information it is automatically packaged and transmitted to the secure private key server 24. A key pair is generated in the secure private key server 24 on receipt of the packaged information and a certificate created using the generated key pair. The certificate is then returned to the applet for onward transmission to the certification authority for signature.

It will be understood that subsequent to correct authentication any further encryption or decryption process requiring the private key will be processed by the secure private key server so that the advantages described continue.

It will further be understood that one form of certificate contains the users identitiy, the users private key and the users public key and that another form contains only the users identity and public key. The certificate containing the users private key is available only to the secure private key server and the other certificate is passed to the applet. It will also be understood that when the vendor sends its certificate to the applet that this does not contain a private key.

It will of course be understood that the invention is not limited to the specific details as herein described, which are given by way of example only, and that various alterations and modifications may be made without departing from the scope of the invention.

CLAIMS:

1. A method for secure data communication for use in an electronic commerce environment of the type having an authentication server (2), a web server (3) and an applet (5) characterised in that the method controls data communications between the authentication server, web server, applet and a secure private key server (4) by performing the steps of: -

downloading the applet from a vendor web site in response to a data communication request;

requesting a copy of a vendor certificate from the web site;

extracting a data response to generate a certificate-received signal;

automatically initiating an authentication request for transmission to the authentication server;

interrogating the authentication server and requesting return transmission of a server authentication certificate;

transmitting a vendor certificate to the applet;

automatically extracting the vendor public key from the vendor certificate within the applet;

loading a client certificate into the applet and simultaneously transmitting the client certificate to the authentication server; and

receiving the client certificate at the authentication server and extracting a client public key from the client certificate and simultaneously

automatically extracting the client public key from the client certificate by the applet.

2. A method as claimed in claim 1 comprising the further steps of: -

initialising the secure private key server;

loading a certificate into the secure private key server;

loading a client private key into the secure private key server;

generating an auto authenticate signal for transmission to the authentication server requesting initialisation of a new authentication process;

retrieving a predefined text string from a local memory using the authentication server and encrypting the text string to generate a cipher text string using the client public key on receipt of the authenticate signal;

transmitting a cipher text string to the applet, receiving the cipher text string from the authentication server and routing the cipher text string to the secure private key server;

decrypting the cipher text string to extract a decrypted text string using the client private key and transferring the decrypted text string to the applet;

encrypting the decrypted text string received from the secure private key server with the vendor public key extracted from the vendor certificate to generate a vendor encoded text string;

sending the vendor encoded text string to the authentication server, decrypting the encoded text string to generate an authentication text string using the vendor private key; and

comparing the authentication text string and the predefined text string to generate a match / no match signal and in response to a no match signal terminating communication or in response to a match signal for further authenticated data communications.

3. A method of generating a certificate operating in a data communication system having a web server, a certification authority, an applet and a secure private key server by performing the steps of: -

gathering certification information in the applet and transmitting the information to the secure private key server;

generating a key pair in the secure private key server on receipt of the packaged information and a certificate created using the generated key pair; and

returning the certificate to the applet for onward transmission to the certification authority for signature.

4. A method substantially as herein described with reference to and as shown in the accompanying drawings.

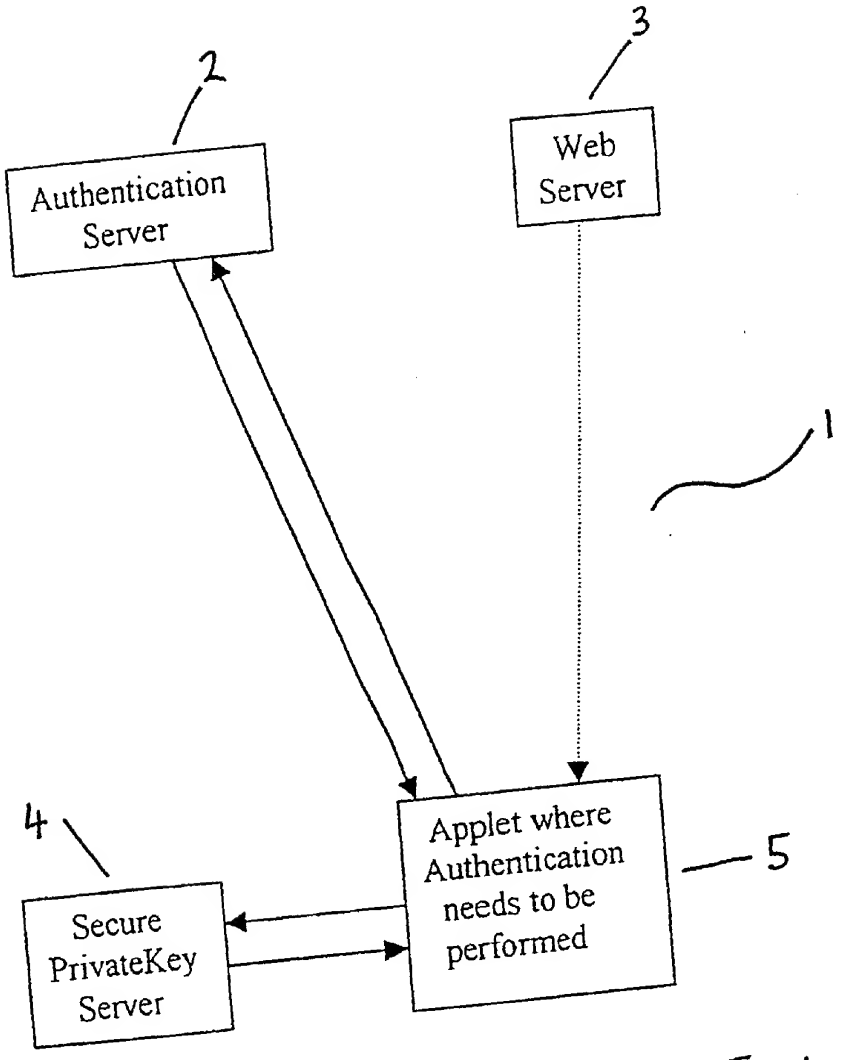

2
Authentication Server
3
Web Server
1
4
Secure PrivateKey Server
Applet where Authentication needs to be performed
5

Fig. 1

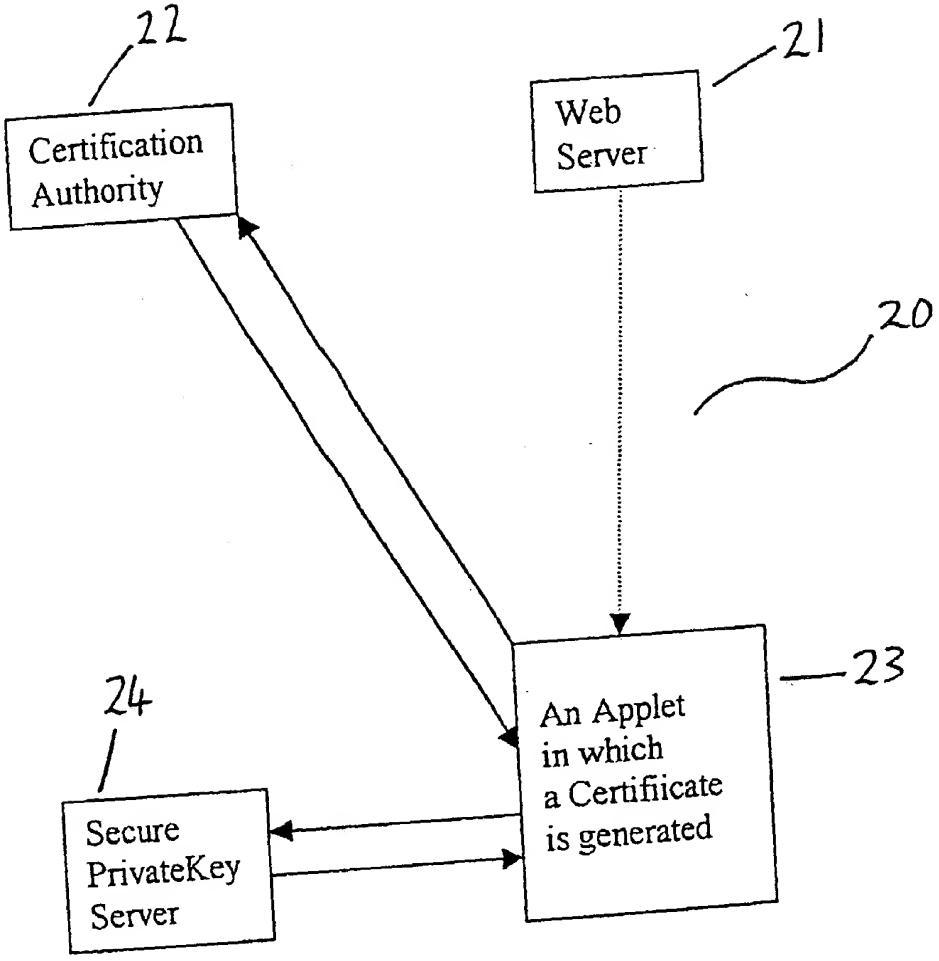

22
Certification Authority
21
Web Server
20
23
An Applet in which a Certifiicate is generated
24
Secure PrivateKey Server

Fig. 2

# INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/IE 00/00050

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 99 05813 A (VISTO CORP)<br>4 February 1999 (1999-02-04)<br>abstract<br>page 2, line 14 -page 3, line 5<br>page 3, line 12 -page 4, line 5<br>page 7, line 5 - line 11<br>page 7, line 21 -page 8, line 5<br>page 8, line 22 -page 9, line 5<br>page 13, line 11 - line 14<br>--- | 1-3 |
| A | EP 0 817 103 A (SUN MICROSYSTEMS INC)<br>7 January 1998 (1998-01-07)<br>abstract<br>page 2, column 2, line 26 -page 3, column 3, line 5<br>page 4, column 6, line 8 - line 41<br>---<br>-/-- | 1-3 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 11 September 2000 | 22/09/2000 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Adkhis, F |

2

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/IE 00/00050

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | PAONE J: "PKI provides a base for secure transactions" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 16, no. 7, 1997, pages 620-621, XP004099324 ISSN: 0167-4048 the whole document | 1-3 |

2

# INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/IE 00/00050

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9905813 A | 04-02-1999 | NONE | |
| EP 0817103 A | 07-01-1998 | US 5953005 A | 14-09-1999 |
| | | JP 10232841 A | 02-09-1998 |